CLAIMS

What is claimed is:

1. A method for summarizing firewall activity, comprising:

(a) organizing a plurality of types of events associated with a firewall of a local computer;

(b) tracking a number of occurrences of each type of event utilizing the firewall; and

(c) displaying a graphical representation indicating a severity of the number of the events utilizing the firewall.

2. The method as recited in claim 1, wherein the events include blocked attempts of various types.

3. The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts of remote computers to access predetermined banned ports associated with the local computer.

4. The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts of remote computers with a predetermined set of Internet Protocol (IP) addresses to access the local computer.

5. The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts to access a network made by predetermined applications.

10074586 - 020802

6. The method as recited in claim1, wherein the displayed number of occurrences of each type of event occurred within a predetermined time period.

7. The method as recited in claim 1, and further comprising displaying additional information relating to the events upon the selection thereof.

8. The method as recited in claim 2, wherein a first type of the blocked attempts includes blocked attempts of remote computers to access predetermined banned ports associated with the local computer, a second type of the blocked attempts includes blocked attempts of the remote computers with a predetermined set of Internet Protocol (IP) addresses to access the local computer, and a third type of the blocked attempts includes blocked attempts to access a network made by predetermined applications.

9. The method as recited in claim 8, wherein the first type of the blocked attempts, the second type of the blocked attempts, and the third type of the blocked attempts are organized into categories.

10. The method as recited in claim 8, wherein a plurality of banned ports associated with the first type of the blocked attempts are displayed with the number of the occurrences associated therewith.

11. The method as recited in claim 8, wherein a plurality of banned IP addresses associated with the second type of the blocked attempts are displayed with the number of the occurrences associated therewith.

12. The method as recited in claim 8, wherein a plurality of banned applications associated with the third type of the blocked attempts are displayed with the number of the occurrences associated therewith.

EDS_1505 - 02/06/02

13. The method as recited in claim 8, and further comprising displaying a menu for selecting from a summary page, an applications page, an event log, and an IP address page.

14. The method as recited in claim 8, and further comprising displaying a menu.

15. The method as recited in claim 14, wherein upon the selection of an applications page on the menu, displaying an applications interface for selecting the predetermined applications.

16. The method as recited in claim 14, wherein upon the selection of an IP address page on the menu, displaying an IP address interface for selecting the predetermined IP addresses associated with the remote computers to be blocked.

17. The method as recited in claim 14, wherein upon the selection of an event log on the menu, displaying a log of the events.

18. The method as recited in claim 1, wherein the graphical representation includes a bar graph.

19. A computer program product for summarizing firewall activity, comprising:
(a) computer code for organizing a plurality of types of events associated with a firewall of a local computer;
(b) computer code for tracking a number of occurrences of each type of event utilizing the firewall; and
(c) computer code for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall.

20. A system for summarizing firewall activity, comprising:

(a) logic for organizing a plurality of types of events associated with a firewall of a local computer;

(b) logic for tracking a number of occurrences of each type of event utilizing the firewall; and

(c) logic for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall.

21 A system for summarizing firewall activity, comprising:

(a) means for organizing a plurality of types of events associated with a firewall of a local computer;

(b) means for tracking a number of occurrences of each type of event utilizing the firewall; and

(c) means for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall.

22. A method for managing a firewall, comprising:

(a) displaying a menu for selecting from a summary page, an applications page, and an Internet Protocol (IP) address page;

(b) upon the selection of the summary page on the menu, displaying a plurality of types of blocked attempts, and an indication as to the number of occurrences of each type of the blocked attempt, wherein a first type of the blocked attempts includes blocked attempts of the remote computers with a predetermined set of Internet Protocol (IP) addresses to access the local computer, and a second type of the blocked attempts includes blocked attempts to access a network made by predetermined applications;

(c) upon the selection of the applications page on the menu, displaying an applications interface for selecting the predetermined applications; and

(d) upon the selection of the IP address page on a menu, displaying an IP address interface for selecting the predetermined IP addresses associated with remote computers to be blocked.

23. A method for managing a firewall and reporting firewall activity associated therewith, comprising:

(a) displaying in a first portion of an event log a plurality of events;

(b) upon the selection of one of the events, displaying in a second portion of the event log information relating to the event; and

(c) displaying a menu in a third portion of the event log a menu for selecting from a summary page for summarizing the events, an application selection page for selection of applications to be subject to security restrictions, and an Internet Protocol (IP) address selection page for selection of IP addresses to be subject to security restrictions.

24. A firewall method, comprising:

(a) executing a firewall in association with a local computer;

(b) identifying a number of blocked attempts of remote computers with a predetermined set of Internet Protocol (IP) addresses to access the local computer;

(c) identifying a number of attempts of the remote computers to access predetermined frequently-used ports associated with the local computer;

(d) identifying a number of blocked attempts to access a network made by predetermined applications on the local computer;

(e) displaying a menu for selecting from a plurality of interface features including a summary page, an applications page, an event log, and an IP address page;

(f) upon the selection of the summary page on the menu,

(i) displaying a recent activity list including recent activity icons corresponding to events including total blocked attempts, the attempts of the remote computers to access the predetermined frequently-used ports associated with the local computer, the blocked attempts of the remote computers with the predetermined set of IP addresses to access the local computer, the recent activity list further including a total number of the events within a predetermined time period

corresponding with each recent activity icon, and a graphical representation indicating a severity of the total number of the events,

(ii) displaying a frequently accessed port list including port icons corresponding to the predetermined frequently-used ports, the frequently accessed port list further including a total number of the attempts corresponding with each predetermined frequently-used ports, and a graphical representation indicating a severity of the total number of the attempts,

(iii) displaying a commonly blocked IP address list including IP address icons corresponding to banned IP addresses from which the blocked attempts of the remote computers occurred, the commonly blocked IP address list further including a total number of the blocked attempts corresponding with each IP address icon, and a graphical representation indicating a severity of the total number of the blocked attempts,

(iv) displaying a commonly blocked application list including application icons corresponding to banned applications associated with the blocked attempts, the commonly blocked application list further including a total number of the blocked attempts corresponding with each application icon, and a graphical representation indicating a severity of the total number of the blocked attempts;

(g) upon the selection of the applications page on the menu, displaying an applications interface for selecting the predetermined applications;

(h) upon the selection of the untrusted IP address page on the menu, displaying an untrusted IP address interface for selecting the IP addresses associated with remote computers to be blocked; and

(i) upon the selection of the event log on the menu, displaying a log of the attempts.

20020085745.001